CLAIMS

We claim:

1. A method for secure access to a computer system, comprising the steps of:

receiving in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function;

determining if said access request completes a prohibited temporal access pattern for said entity; and

comparing a minimum access level established for said first base node to said predetermined access level; and

granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

2. The method according to claim 1, further comprising the step of denying said request if said access request completes a prohibited temporal access pattern for said entity.

3. The method according to claim 1, further comprising the step of denying said request if said minimum access level for said first base node exceeds said predetermined access level for said entity.

4. The method according to claim 1, further comprising the steps of:

logically organizing said computer system in the form of a tree hierarchy having a plurality of leaf nodes and higher-level nodes;

defining a plurality of said base nodes as comprising respectively a plurality of leaf nodes of said tree hierarchy; and

defining said higher-level nodes as aggregations of said base nodes.

5. The method according to claim 4 further comprising the step of identifying within said hierarchy any higher-level nodes that are aggregations comprising said first base node.

6. The method according to claim 5, further comprising the step of identifying within said hierarchy any nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

7. The method according to claim 6, further comprising the step of updating a minimum required entity access level for any base nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

8. The method according to claim 7, wherein said updating step further comprises the steps of:

comparing said entity's predetermined access level against the minimum required access level of said higher-level nodes that are aggregations comprising said first base node; and

updating a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.

9. The method according to claim 1, further comprising the steps of:

comparing said entity's predetermined access level against the minimum required access level of at least one higher-level node that is an aggregation of base nodes including said first base node; and

updating a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.

10. A method for restricting access to a computer system having a plurality of logical base nodes representing at least one of an information type and a computer system function, and a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy, comprising the steps of:

receiving in said computer system a request from an entity with a predetermined access level for access to a first base node;

determining if said access request completes a prohibited temporal access pattern for said entity; and

comparing a minimum access level established for said first base node to said predetermined access level; and

granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

11. A secure computer system comprising:

a plurality of logical base nodes representing at least one of an information type and a computer system function;

a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy;

a computer system interface capable of receiving a request from an entity with a predetermined access level for access to a first base node;

a temporal access table;

processing means programmed for comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity, and for comparing a minimum access level established for said first base node to said predetermined access level; and

wherein said processing means grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

12. The secure computer system according to claim 11, wherein said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity.

13. The secure computer system according to claim 11, wherein said processing means denies said request if said minimum access level for said first base node exceeds said predetermined access level for said entity.

14. The secure computer system according to claim 11 wherein said higher-level nodes are aggregations of said base nodes.

15. The secure computer system according to claim 14 wherein said processing means identifies within said hierarchy any higher-level nodes that are aggregations comprising said first base node.

16. The secure computer system according to claim 15 wherein said computer processing means identifies within said hierarchy any nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

17. The secure computer system according to claim 16 wherein said processing means updates a minimum required entity access level for any base nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

18. The secure computer system according to claim 17 wherein said processing means compares said entity's predetermined access level against the minimum required access level of said higher-level nodes that are aggregations comprising said first base node; and

automatically updates a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.

19. The secure computer system according to claim 11 wherein said processing means compares said entity's predetermined access level against the minimum required access level of at least one higher-level node that is an aggregation of base nodes including said first base node; and

updates a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.